Chow Min Po

From: Chen Tai Pang
Sent: Monday, October 22, 2001 2:58 PM
To: Chow Min Po
Cc: Yau Wei Yun
Subject: Submission of a Initial Patent Write-up
Importance: High

Dear Cecilia,

I and Dr. Yau Wei Yun would like to patent an invention. We would like to submit an initial patent write-up to the patent approval committee. The inventors of this patent are me (CHEN Tai Pang) and Dr. Yau Wei Yun. The title of our invention is "Authentication Processing on a Resource Constrained Processing Platform". Please contact me or Wei Yun, if you have any problem regarding to our patent write-up. I attached a copy of Initial Patent Write-up with the email.

Regards,
Lawrence CHEN.

38

INITIAL PATENT WRITE-UP

(Please keep the length of answers to questions 1,2 and 3 to about half a page)

Patent Ref. No: CSP/PAT/01/015

Name of Inventor(s): CHEN Tai Pang, YAU Wei Yun

TITLE OF INVENTION

Authentication Processing on a Resource Constrained Processing Platform

1. WHAT IS THE INVENTION?

(Describe briefly what the invention is about, and how it is different from what is available)

In this disclosure, a new methodology of performing identification using biometric on resource-constrained platform such as smart card is proposed. It is widely recognized that biometrics is a better identity authentication method than using PIN or password. However, because of the limited resources in a smart card, it is commonly used only to store the biometric templates. This is not as secure because an attacker can emulate the smart card and its reader. A better approach is to perform the matching on the smart card itself so that the template stored in the smart card is never revealed. However, such processing is typically long and cannot be completed within the 2 sec requirement (which is the rule of thumb in the financial industry for any ATM transaction).

The invention disclosed here proposed a method to allow distributed processing between the smart card and the client (which is usually the PC). An example implementation of fingerprint matching on smart card is proposed. However, the approach can be extended to any implementation, including to perform the entire fingerprint matching on smart card. The proposed method will always be useful because processing power of the smart card (or any resource constrained device) will always lag behind the PC (or any server) by a huge magnitude (today, most smart card is using only an 8-bit processor running at about 10MHz compared to the PC which is 32-bit running at over 1GHz). In other words, the proposed method provides a means for any resource-constrained device to perform a much more computationally intensive task and without requiring a high speed/bandwidth communication that is required by today's client-server and distributed processing architecture.

In addition to the ability of performing matching on smart card, this invention proposed a novel way of communicating to the client the results of the matching using a string of numbers, called Unique Identification Number (UIN). The UIN will contain the results of the matching, together with identifier and a randomly number. The UIN will be changed every time the system is accessed, giving it a life-span of single use (similar to one-time password). This will allow proper decision to be made by the client in a secure manner without depending too much on the encryption capability. Even if the system is compromised, the UIN is able to tell that the system has been hacked.

In summary, this invention consists of the following features:
(1) Protocols to control on card fingerprint matching and transaction.
(2) The Unique personal Identification Number (UIN) holds the identifier and matching results and hides the security access code that avoids intruder access.
(3) One-time password like protocol for keeping track of UIN.
(4) The method of Distributed Remote Execution, which performs load sharing, resolves the problem of resource-constrained device such as the smart card to perform compute-intensive tasks.

2. WHAT IS NEW ABOUT THE INVENTION?

(Establish the novelty of the invention. Is there any prior art to the invention? Has the invention ever being made known to the public in any ways?)

No prior art has been found. Most of the prior inventions were using PIN as the key of verification. Such as the VISA Cash system, it uses multiple authentication keys to request for a single transaction. And all these inventions heavily rely on standard cryptograph for protecting data security. Even if biometrics is used, it is confined to identity authentication and the results made known to the server. There is no tight integration with biometrics. Our invention is different in that the smart card acts as both a biometric agent and a transaction agent, giving it a tight integration. The biometric agent is responsible for authenticating the user while the transaction agent is responsible for conducting transaction with the remote transaction server. A secured interface was defined for both agents. The biometric agent can alter the states of the transaction agent but not vice versa.

There have also been numerous patents on the use of smart card to store the fingerprint template and also to perform the whole of matching on smart card. Our invention is different in that it proposed a method of partial matching on the smart card. A new protocol was defined which combines the security nature of the smart card with the high processing speed of the remote clients without compromising the reliability of the templates. In addition, the proposed protocol, unlike the existing client server or distributed processing protocol, does not require high-speed connection or huge memory. The protocol can support multiple servers. Thus the protocol allows a resource-constrained device to execute a transaction with load sharing with a server at an acceptable speed and with high security.

Given that the smart card is able to perform the matching on card, most existing solutions merely send the matching result via cookies or a long transaction key to the server with encryption. Thus the security depends a lot on the encryption – if the encryption fails, then the system is compromised. Our invention is different in that we proposed a method to synthesize the identifier number with biometrics matching score and a random number to allow for identity authentication, access privilege and policy. The UIN is also changed for every valid transaction and thus it gives high security without totally relying on encryption technology. Even if the system is compromised, the user will be aware of it by the very nature of the proposed UIN protocol.

3. WHAT IS GOOD ABOUT THE INVENTION?

(What is its commercial value? How much better is it compared to the best in the world?)

According to the security certification, ability to perform the complete processing on smart card has the highest security rating, followed by performing biometric matching on smart card and then using smart card to store the template. Our invention allows both the complete biometric processing on smart card and matching on smart card to be computationally viable without compromising the security level. Furthermore, since the solution does not depend on high-speed communication, it is applicable to any resource-constrained device. There are huge demand such as handphone and pda as the computational power of these devices will always lack behind the server in many folds. Such capability will also allow a future generation of mobile device that is very compact, low cost, low computational power and has connection to a server. Such a device can be distributed free while the company earns the money through subscription services to the server and the transaction cost as well as the amount of data transmitted. Such a model will make the practice of giving away free handphones more widespread. And these handphones need not be limited in computational capability.

In addition, with the ability of matching on smart card, the results are transmitted via the proposed UIN. Such invention provides the ability of identity authentication and is independent of the types of biometrics -- thus giving it a good way of providing interoperability. The fact that the UIN varies at every successful access, which is similar to one-time password, gives it a good security and is not totally dependent on the performance of the encryption system. Thus security level is very high.

The combined invention has many interesting applications. An example is that a pda with fingerprint sensor and infra-red communication can open a door. The door only needs to have a micro-controlled with infra-red communication capability. The handphone will perform the feature extraction which will then perform the matching together with the SIM card. The SIM card then computes the UIN which is transmitted to the door's micro-controller (the handphone must be pre-registered with the doors's micro-controller). If the UIN matches to a certain degree, access will be granted and the UIN updated at both the door and the handphone. At the next access, the same UIN as the previous one will not be able to open the door. Such a system is interesting in the following aspects:

1. One only needs a mobile device (ex: handphone, pda, keyfob etc) that can be used for many controllers (ex: all door-locks, drawer-locks, PCs etc).
2. Each controller does not require a powerful micro-controller to perform the fingerprint processing and the sensor, making it very simple, small and extremely cheap.
3. The ever changing UIN does not require very secure encryption. This is an important factor as the ease of breaking an encryption algorithm increases with time as the computational power of CPU keeps on increasing and the danger of the availability of quantum computers.

This invention arises due to the queries from companies such as Moneyhive, Sensecurity and Infineon. The proposed system can find implementation in many areas. Recently, Infineon has approached us to collaborate on a secure USB dongle. The USB dongle will contain a fingerprint sensor, micro-controller and memory. The processing will fit nicely using the invention that we have proposed. X-Bio is keen on this project and they are targeting customers including MINDEF and government agencies for confidential applications. Two applications have been suggested (which we cannot disclose due to its confidential nature). There will be many more opportunities available in the future for this invention.

Confidential

CENTRE FOR SIGNAL PROCESSING

Patent Filing Approval Form

(PFA)

Patent Ref.No.: CSP/PAT/01/015
(This number will be assigned by the Administrator)

☐ Please tick where appropriate.

Please ensure Fields 1 to 7 is completed, and the **Initial Patent Write-up and Search Report are attached in a sealed envelope** before passing to the BDO and state NIL where applicable.

1. Patent Title: **Authentication Processing on a Resource Constrained Processing Platform**

2. Name of Inventor(s): **Chen Tai Pang, Yau Wei Yun**

3. Core Technology Area: ☐ Audio Processing ☐ Speech Processing ☐ Image & Video Processing ☐ Adaptive Signal Processing ☐ DSP Hardware & Implementation ☒ Others Biometrics

4. Program: ☐ Multi-Media System ☐ Multi-Media Coding ☐ Video Processor ☐ Special Effects ☐ Voice Based Biometrics ☒ Image Based Biometrics ☐ Others _____

5. Assistance from BDO

☑ To assist in contacting patent attorney

☐ To assist in reviewing the non-technical aspects of Final Patent Write-up

6. Prior Art Search

I have done the prior art search on the invention at the following website: WWW.USPTO.ORG

_____

7. Submitted by Inventor(s):
CHEN TAI PANG 22/10/2001

_____
Names & Signature + Date

8. Approval granted/~~Rejected~~* by:

30/1/2002

_____
Director + Date

FOR OFFICIAL USE ONLY

9. Filing destination
☐ Singapore Only ☐ PCT ☐ Other Country(s) : _____

10. Remarks (if any)

*Please delete accordingly

Please submit the completed form, together with the write-up and search report to Cecilia

Confidential

PFA No.: **CSP/PAT/01/015**
Patent: **Authentication Processing on a Resource Constrained Processing Platform**
Inventor(s): **Chen Tai Pang, Yau Wei Yun**

		Yes	Date	To file?
1	Submitted PFA with Initial Write-up and Search Report?	✓	22 Mar 02	
2	Distributed to Review Committee?	✓	25 Mar 02	
	Review Committee Meeting	✓	27 Mar 02	
	Review Committee Group (1 or 2)			
	Outcome: Send questions to inventors.			
3	List of queries sent to inventor for clarifications?	✓	28 Mar 2002	
	Received answers from inventors?	✓	29 Mar 02	
	Sent answers to review committee via email?	✓	30 Mar 02	
4	2nd Review Committee Meeting	✓	30 Mar 02	
	Outcome: Proceed filing			
5	Patent Agent? Wong & Co.			
	Inventor meeting with PA?			
6	Patent File? Reference no:			

Awaiting final write-up from inventors